CLAIMS

What is claimed is:

1. A method for controlling access rights of a requesting principal to a protected resource in a computer system, wherein a principal is associated with at least one role, the method comprising:

associating a role filter with a role;

associating a set of one or more capabilities with the role;

associating a capability filter with a capability in the set of one or more capabilities; and

authorizing access for the requesting principal to the protected resource based on an association between the requesting principal and the role and based on an association between the protected resource and a capability of the role.

2. The method of claim 1 further comprising:

evaluating the role filter to determine a set of one or more principals to be associated with the role; and

evaluating the capability filter to determine a set of one or more resources to be associated with the capability.

3. The method of claim 1 further comprising:

associating a resource type with each capability in the set of one or more capabilities, wherein each capability defines access to at least one resource of the resource type.

4. The method of claim 1 further comprising:

associating a set of one or more access conditions with each capability in the set of one or more capabilities, wherein each access condition defines an access constraint against authorizing access for the requesting principal to the protected resource.

5. The method of claim 4 further comprising:

associating a set of one or more rights with each access condition in the set of one or more access conditions, wherein each right defines an access type for authorized access for the requesting principal to the protected resource.

6. The method of claim 1 further comprising:

associating a filterRoles list with the requesting principal, wherein the filterRoles list is a multivalued attribute containing a set of one or more roles;

associating a filterMembers list with the role, wherein the filterMembers list is a multivalued attribute containing a set of one or more principals;

adding the role to the filterRoles list associated with the requesting principal if the requesting principal is added to the filterMembers list associated with the role; and

adding the requesting principal to the filterMembers list associated with the role if the role is added to the filterRole list associated with the requesting principal.

7. The method of claim 1 further comprising:

associating a filterCapabilities list with a resource, wherein the filterCapabilities list is a multivalued attribute containing a set of one or more capabilities;

associating a filterTargets list with a capability, wherein the filterTargets list is a multivalued attribute containing a set of one or more resources;

adding the capability to the filterCapabilities list associated with the resource if the resource is added to the filterTargets list associated with the capability; and

adding the resource to the filterTargets list associated with the capability if the capability is added to the filterCapabilities list associated with the resource.

8. The method of claim 1 further comprising:

receiving notification of an update to an instance, wherein the instance has a type selecting from the group of "principal", "resource", "capability", or "role";

determining the type of the instance;

searching for capabilities with a resource type that matches the type of the instance; and

running capability filters of matched capabilities against the instance.

9. The method of claim 8 further comprising:

in response to a determination that the type of the instance is "principal", running all role filters against the instance.

10. The method of claim 9 further comprising:

in response to a determination that the type of the instance is "role" or "capability", determining whether a filter of the instance has been updated; and

in response to a determination that the filter of the instance has been updated, running the filter of the instance in accordance with the type of the instance.

11. An apparatus for controlling access rights of a requesting principal to a protected resource in a computer system, wherein a principal is associated with at least one role, the apparatus comprising:

means for associating a role filter with a role;

means for associating a set of one or more capabilities with the role;

means for associating a capability filter with a capability in the set of one or more capabilities; and

means for authorizing access for the requesting principal to the protected resource based on an association between the requesting principal and the role and based on an association between the protected resource and a capability of the role.

12. The apparatus of claim 11 further comprising:

means for evaluating the role filter to determine a set of one or more principals to be associated with the role; and

means for evaluating the capability filter to determine a set of one or more resources to be associated with the capability.

13. The apparatus of claim 11 further comprising:

means for associating a resource type with each capability in the set of one or more capabilities, wherein each capability defines access to at least one resource of the resource type.

14. The apparatus of claim 11 further comprising:

means for associating a set of one or more access conditions with each capability in the set of one or more capabilities, wherein each access condition defines an access constraint against authorizing access for the requesting principal to the protected resource.

15. The apparatus of claim 14 further comprising:

means for associating a set of one or more rights with each access condition in the set of one or more access conditions, wherein each right defines an access type for authorized access for the requesting principal to the protected resource.

16. The apparatus of claim 11 further comprising:

means for associating a filterRoles list with the requesting principal, wherein the filterRoles list is a multivalued attribute containing a set of one or more roles;

means for associating a filterMembers list with the role, wherein the filterMembers list is a multivalued attribute containing a set of one or more principals;

means for adding the role to the filterRoles list associated with the requesting principal if the requesting principal is added to the filterMembers list associated with the role; and

means for adding the requesting principal to the filterMembers list associated with the role if the role is added to the filterRole list associated with the requesting principal.

17. The apparatus of claim 11 further comprising:

means for associating a filterCapabilities list with a resource, wherein the filterCapabilities list is a multivalued attribute containing a set of one or more capabilities;

means for associating a filterTargets list with a capability, wherein the filterTargets list is a multivalued attribute containing a set of one or more resources;

means for adding the capability to the filterCapabilities list associated with the resource if the resource is added to the filterTargets list associated with the capability; and

means for adding the resource to the filterTargets list associated with the capability if the capability is added to the filterCapabilities list associated with the resource.

18. The apparatus of claim 11 further comprising:

means for receiving notification of an update to an instance, wherein the instance has a type selecting from the group of "principal", "resource", "capability", or "role";

means for determining the type of the instance;

means for searching for capabilities with a resource type that matches the type of the instance; and

means for running capability filters of matched capabilities against the instance.

19. The apparatus of claim 18 further comprising:

means for running all role filters against the instance in response to a determination that the type of the instance is "principal".

20. The apparatus of claim 19 further comprising:

means for determining whether a filter of the instance has been updated in response to a determination that the type of the instance is "role" or "capability"; and

means for running the filter of the instance in accordance with the type of the instance in response to a determination that the filter of the instance has been updated.

21. A computer program product in a computer readable medium for use in a data processing system for controlling access rights of a requesting principal to a protected resource, wherein a principal is associated with at least one role, the computer program product comprising:

instructions for associating a role filter with a role;

instructions for associating a set of one or more capabilities with the role;

instructions for associating a capability filter with a capability in the set of one or more capabilities; and

instructions for authorizing access for the requesting principal to the protected resource based on an association between the requesting principal and the role and based on an association between the protected resource and a capability of the role.

22. The computer program product of claim 21 further comprising:

instructions for evaluating the role filter to determine a set of one or more principals to be associated with the role; and

instructions for evaluating the capability filter to determine a set of one or more resources to be associated with the capability.

23. The computer program product of claim 21 further comprising:

instructions for associating a resource type with each capability in the set of one or more capabilities, wherein each capability defines access to at least one resource of the resource type.

24. The computer program product of claim 21 further comprising:

instructions for associating a set of one or more access conditions with each capability in the set of one or more capabilities, wherein each access condition defines an access constraint against authorizing access for the requesting principal to the protected resource.

25. The computer program product of claim 24 further comprising:

instructions for associating a set of one or more rights with each access condition in the set of one or more access conditions, wherein each right defines an access type for authorized access for the requesting principal to the protected resource.

26. The computer program product of claim 21 further comprising:

instructions for associating a filterRoles list with the requesting principal, wherein the filterRoles list is a multivalued attribute containing a set of one or more roles;

instructions for associating a filterMembers list with the role, wherein the filterMembers list is a multivalued attribute containing a set of one or more principals;

instructions for adding the role to the filterRoles list associated with the requesting principal if the requesting principal is added to the filterMembers list associated with the role; and

instructions for adding the requesting principal to the filterMembers list associated with the role if the role is added to the filterRole list associated with the requesting principal.

27. The computer program product of claim 21 further comprising:

instructions for associating a filterCapabilities list with a resource, wherein the filterCapabilities list is a multivalued attribute containing a set of one or more capabilities;

instructions for associating a filterTargets list with a capability, wherein the filterTargets list is a multivalued attribute containing a set of one or more resources;

instructions for adding the capability to the filterCapabilities list associated with the resource if the resource is added to the filterTargets list associated with the capability; and

instructions for adding the resource to the filterTargets list associated with the capability if the capability is added to the filterCapabilities list associated with the resource.

28. The computer program product of claim 21 further comprising:

instructions for receiving notification of an update to an instance, wherein the instance has a type selecting from the group of "principal", "resource", "capability", or "role";

instructions for determining the type of the instance;

instructions for searching for capabilities with a resource type that matches the type of the instance; and

instructions for running capability filters of matched capabilities against the instance.

29. The computer program product of claim 28 further comprising:

instructions for running all role filters against the instance in response to a determination that the type of the instance is "principal".

30. The computer program product of claim 29 further comprising:

instructions for determining whether a filter of the instance has been updated in response to a determination that the type of the instance is "role" or "capability";

instructions for running the filter of the instance in accordance with the type of the instance in response to a determination that the filter of the instance has been updated.